IMBAUAN KEAMANAN KERENTANAN *REMOTE CODE EXECUTION* PADA WEBMIN (CVE-2022-36446)

Senin, 22 Agustus 2022

Ringkasan Eksekutif

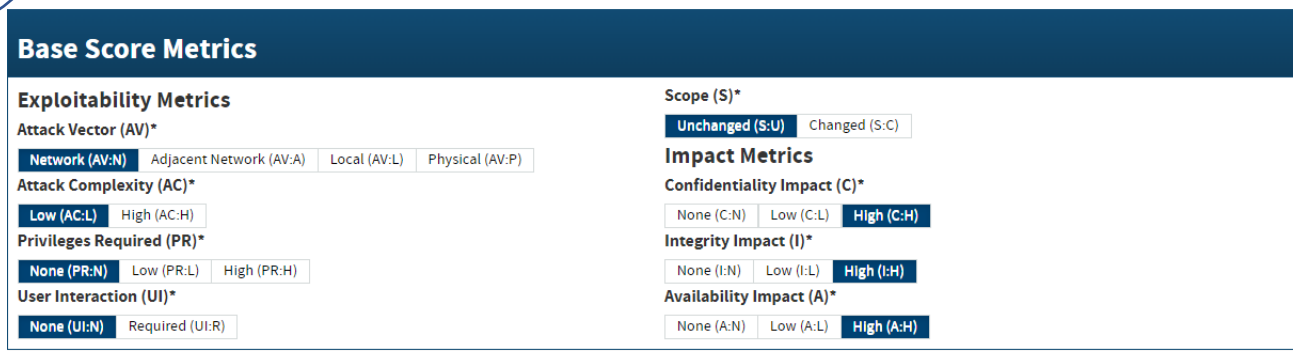
1. Pada 25 Juli 2022, *National Vulnerabilities Database* (NVD) telah mempublikasi imbauan keamanan mengenai kerentanan *software/apt-lib.pl in Webmin before 1.997 lacks HTML escaping for a UI command* yang dapat dieskalasi menjadi *Remote Code Execution (RCE).*
2. Kerentanan ini dideskripsikan pada CVE-2022-36446 sebagai kerentanan yang memiliki dampak *Critical* dengan nilai 9.8.
3. Mengingat dampak yang mungkin muncul dari eksploitasi kerentanan ini, diharapkan pengguna dari produk terdampak untuk segera melakukan tindakan-tindakan mitigasi yang dijelaskan pada imbauan keamanan ini.

Pendahuluan

Webmin adalah panel kontrol manajemen server berbasis *web* yang *powerful* dan fleksibel untuk sistem menyerupai Unix. Webmin memungkinkan pengguna untuk mengkonfigurasi sistem operasi, seperti *user*, *disk*, layanan atau *file* konfigurasi lainya, serta memodifikasi dan mengontrol aplikasi *open-source*, seperti Apache HTTP Server, PHP atau MySQL. Berdasarkan CVE-2022-36446 dapat dilakukan eksploitasi injeksi perintah arbitrer dalam versi Webmin sebelum 1.997. Webmin menggunakan manajer *package* OS (apt, yum, dll.) untuk melakukan pembaruan dan penginstalan *package*. Karena kurangnya sanitasi input, dimungkinkan untuk menginputkan perintah arbitrer yang akan digabungkan ke *package manager*. Eksploitasi ini memerlukan otentikasi dan akun harus memiliki akses ke modul Pembaruan *Package* Perangkat Lunak.

Nilai Kerentanan

Berdasarkan CVSS 3.1, kerentanan ini memiliki nilai **9.8** yang dideskripsikan dengan **CVE-2022-36446** dan dikategorikan sebagai ***Critical*.**



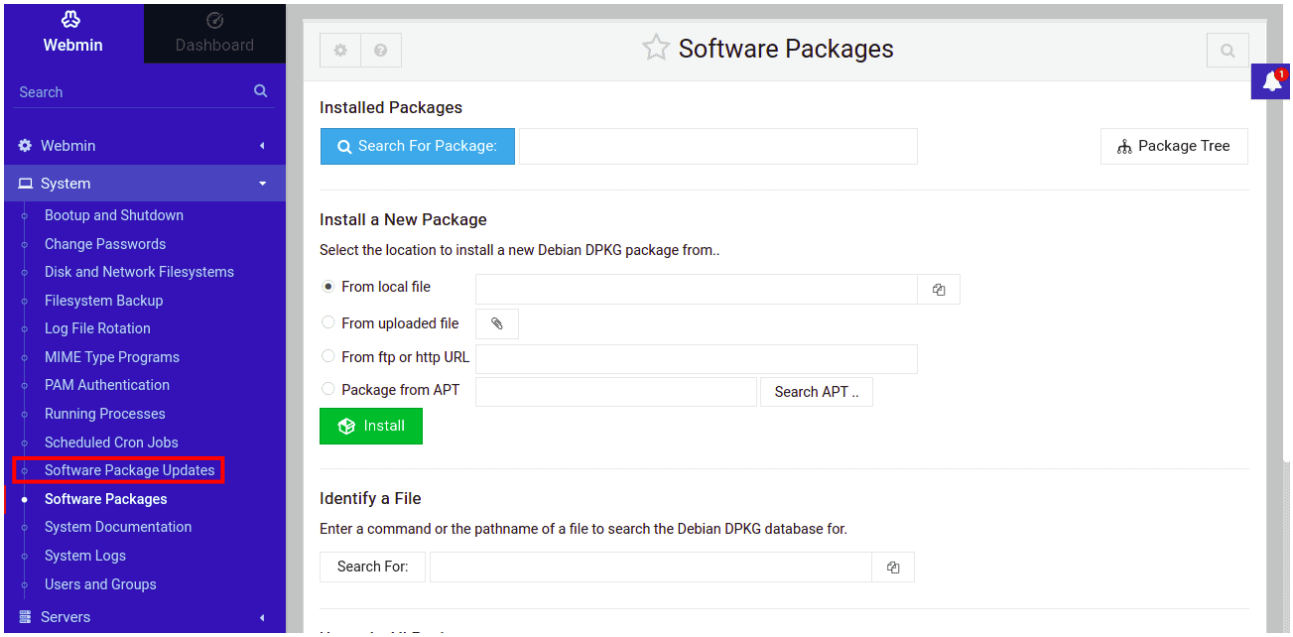
Gambar 1. *Base Score* untuk Kerentanan CVE-2022-36446
Vector String (CVSS:3.1 AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

Produk Terdampak

Produk yang terdampak oleh CVE-2022-36446 ditemukan pada produk Webmin versi 1.996 dan versi sebelumnya.

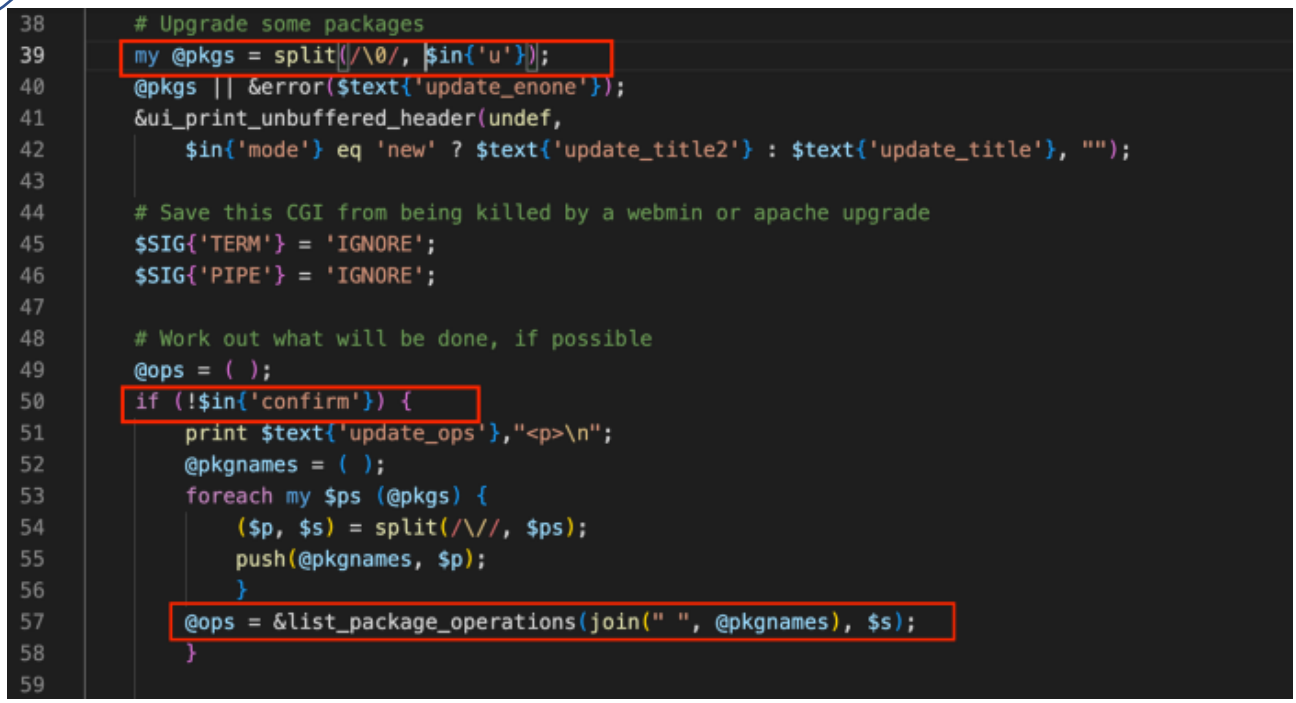
Detail dan Dampak Kerentanan

Untuk mengeksploitasi kerentanan ini, pengguna harus memiliki akses ke modul "*Software Package Updates*".



Gambar 1. *Software Package Updates Module In Webmin Web Interface*

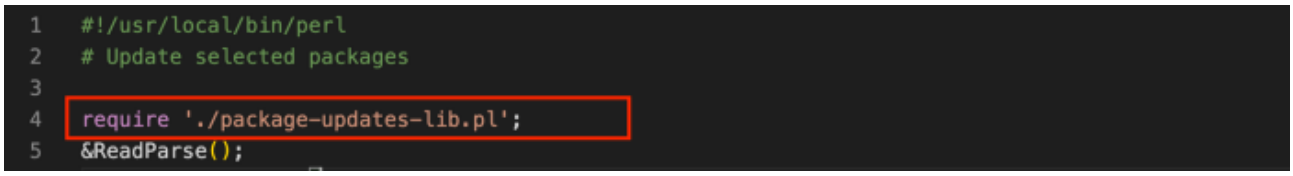
Modul yang dianggap rentan dikembangkan pada "/*package-updates*/". Ketika melihat struktur umum modul *software update packages*, *file* pertama yang harus diamati adalah *file* "update.cgi". Saat melakukan pembaruan *package* atau penginstalasian *package* baru, akan terdapat parameter "u" dalam *request*. Pengguna dapat menemukan parameter "u" yang di *file* "update.cgi" yang telah disebutkan.



```
38      # Upgrade some packages
39      my @pkgs = split(/\0/, $in{'u'});
40      @pkgs || &error($text{'update_enone'});
41      &ui_print_unbuffered_header(undef,
42          $in{'mode'} eq 'new' ? $text{'update_title2'} : $text{'update_title'}, "");
43
44      # Save this CGI from being killed by a webmin or apache upgrade
45      $SIG{'TERM'} = 'IGNORE';
46      $SIG{'PIPE'} = 'IGNORE';
47
48      # Work out what will be done, if possible
49      @ops = ( );
50      if (!$in{'confirm'}) {
51          print $text{'update_ops'},"<p>\n";
52          @pkgnames = ( );
53          foreach my $ps (@pkgs) {
54              ($p, $s) = split(/\//, $ps);
55              push(@pkgnames, $p);
56              }
57          @ops = &list_package_operations(join(" ", @pkgnames), $s);
58          }
59
```

Gambar 2. /package-updates/update.cgi

Seperti pada gambar di atas, *file* mengambil parameter "u" (baris 39) yang menentukan nama *package* dari pengguna dan memeriksa apakah parameter "*confirm*" (baris 50) ada dalam *request*. Jika tidak ada parameter "*confirm*" dalam *request*, sistem akan memanggil fungsi "list_package_operations()" dengan variabel "pkgnames", yang menyimpan nama *package* (baris 57). Fungsi "*list_package_operations*()" ada di *file* "*update*.cgi" -> "*package-updates*-lib.pl" -> "*list_package_operations*()".



```
1   #!/usr/local/bin/perl
2   # Update selected packages
3
4   require './package-updates-lib.pl';
5   &ReadParse();
```

Gambar 3. */package-updates/update.cgi*

```
405  # list_package_operations(package|packages, system)
406  # Given a package (or space-separate package list), returns a list of all
407  # dependencies that will be installed
408  sub list_package_operations
409  {
410  my ($name, $system) = @_;
411  if (defined(&software::update_system_operations)) {
412      my @rv = &software::update_system_operations($name);
413      foreach my $p (@rv) {
414          $p->{'system'} = $system;
415          }
416      return @rv;
417      }
418  return ( );
419  }
420
```

Gambar 4. */package-updates/package-updates-lib.pl*

Fungsi ini mengirimkan nilai "$*name*", yaitu nama *package*, ke fungsi "*update_system_operations()"* dalam *file* bernama "*software*" *foreign* di baris 412. Selanjutnya perlu diketahui di mana fungsi ini didefinisikan. Hal tersebut dapat ditemukan pada *file* di mana fungsi ini didefinisikan dengan menggunakan fitur pencarian di *code editor* (VSCode). "apt-lib.pl" dan "yum-lib.pl". Memahami dari konvensi penamaan bahwa *file* "apt-lib.pl" akan menggunakan *package* "apt", dan *file* "yum-lib.pl" akan menggunakan *package* "yum". Dengan kata lain, pekerjaan yang dilakukan oleh keduanya sama, tetapi karena sistem yang menjalankan Webmin dan *package manager* dari sistem itu berbeda, hanya perintah yang akan berubah. Pengujian dilakukan pada sistem Ubuntu. Oleh karena itu, akan lebih akurat untuk memeriksa *file* "apt-lib.pl".

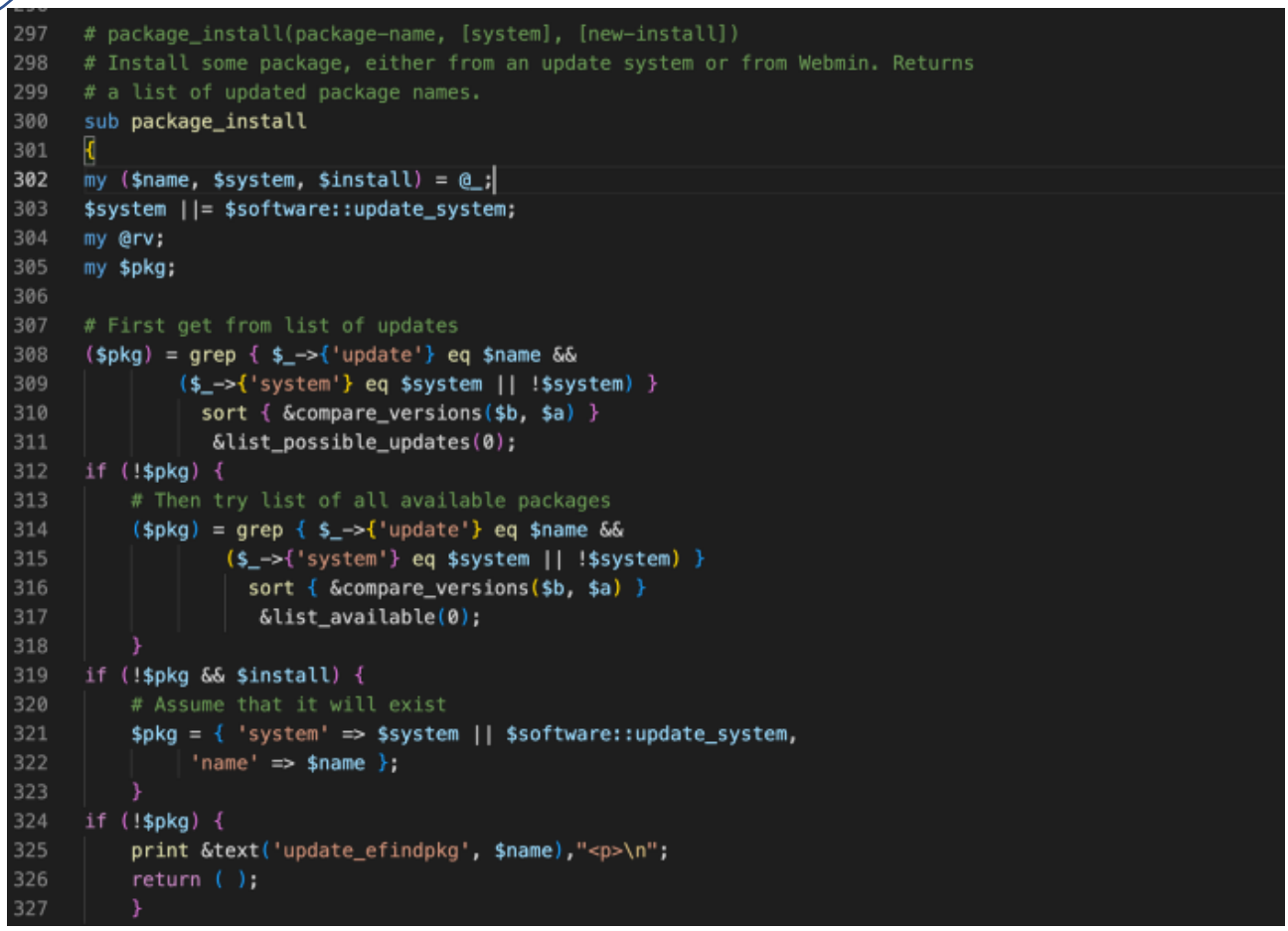
```
72  # update_system_operations(packages)
73  # Given a list of packages, returns a list containing packages that will
74  # actually get installed, each of which is a hash ref with name and version.
75  sub update_system_operations
76  {
77  my ($packages) = @_;
78  $ENV{'DEBIAN_FRONTEND'} = 'noninteractive';
79  my $cmd = "apt-get -s install ".
80        join(" ", map { quotemeta($_) } split(/\s+/, $packages)).
81        " </dev/null 2>&1";
82  &clean_language();
83  my $out = &backquote_command($cmd);
84  &reset_environment();
85  my @rv;
```

Gambar 5. */software/apt-lib.pl*

ketika melakukan akses isi *file* “apt-lib.pl”, pengguna dapat melihat bahwa fungsi *“update_system_opeartions*()” (baris 75) didefinisikan dan mulai menjalankan perintah pada sistem. Terlihat pada gambar diatas, perintah dijalankan dengan fungsi “&*backquote_command*()”. Dari konvensi penamaan bahwa perintah yang dijalankan pada sistem dikontrol dengan aman dalam fungsi ini dan pengguna dicegah untuk memasukkan perintah. Kembali pada *update* “*update*.cgi”, pada intinya untuk kasus di mana parameter "*confirm*" tidak diminta selama instalasi *package*. Bagaimana jika pengguna mengirim parameter "*confirm*" dalam permintaan.

Gambar 6. */package-updates/update.cgi*

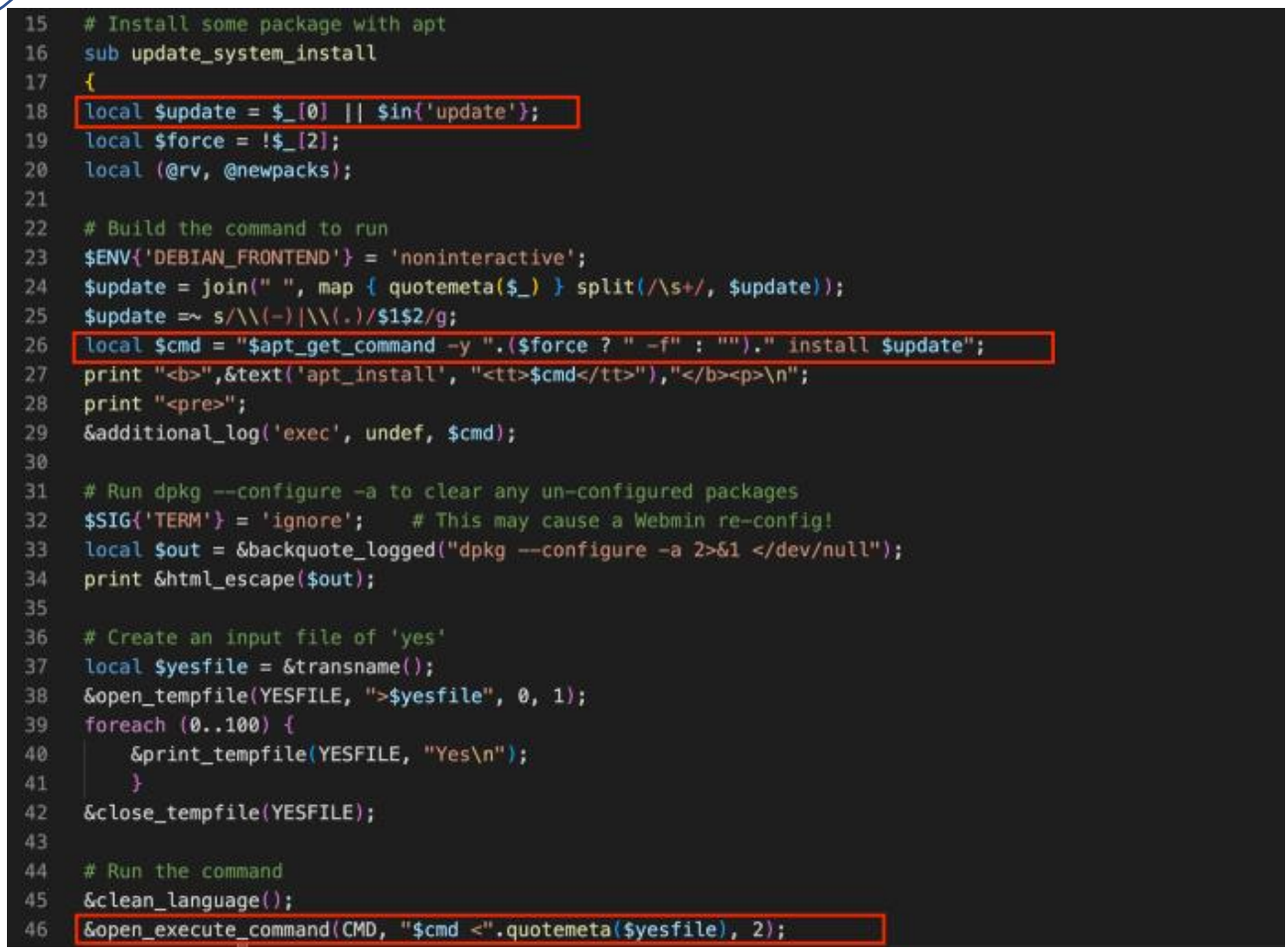
Pada “*update.cgi*”, dapat dilihat bahwa fungsi “*package_install*()” digunakan pada baris 129 jika sebuah *package* akan diinstal, selain dari blok *if* dimana parameter “*confirm*” yang diperiksa pertama kali. Sama seperti langkah sebelumnya di atas, untuk menemukan fungsi ini, pengguna masuk ke *file* “*package-updates-lib.pl*” dan melihat isi dari fungsi tersebut.



```
297  # package_install(package-name, [system], [new-install])
298  # Install some package, either from an update system or from Webmin. Returns
299  # a list of updated package names.
300  sub package_install
301  {
302  my ($name, $system, $install) = @_;
303  $system ||= $software::update_system;
304  my @rv;
305  my $pkg;
306
307  # First get from list of updates
308  ($pkg) = grep { $_->{'update'} eq $name &&
309          ($_->{'system'} eq $system || !$system) }
310            sort { &compare_versions($b, $a) }
311             &list_possible_updates(0);
312  if (!$pkg) {
313      # Then try list of all available packages
314      ($pkg) = grep { $_->{'update'} eq $name &&
315               ($_->{'system'} eq $system || !$system) }
316                sort { &compare_versions($b, $a) }
317                 &list_available(0);
318      }
319  if (!$pkg && $install) {
320      # Assume that it will exist
321      $pkg = { 'system' => $system || $software::update_system,
322           'name' => $name };
323      }
324  if (!$pkg) {
325      print &text('update_efindpkg', $name),"<p>\n";
326      return ( );
327      }
```

Gambar 7. */package-updates/package-updates-lib.pl*

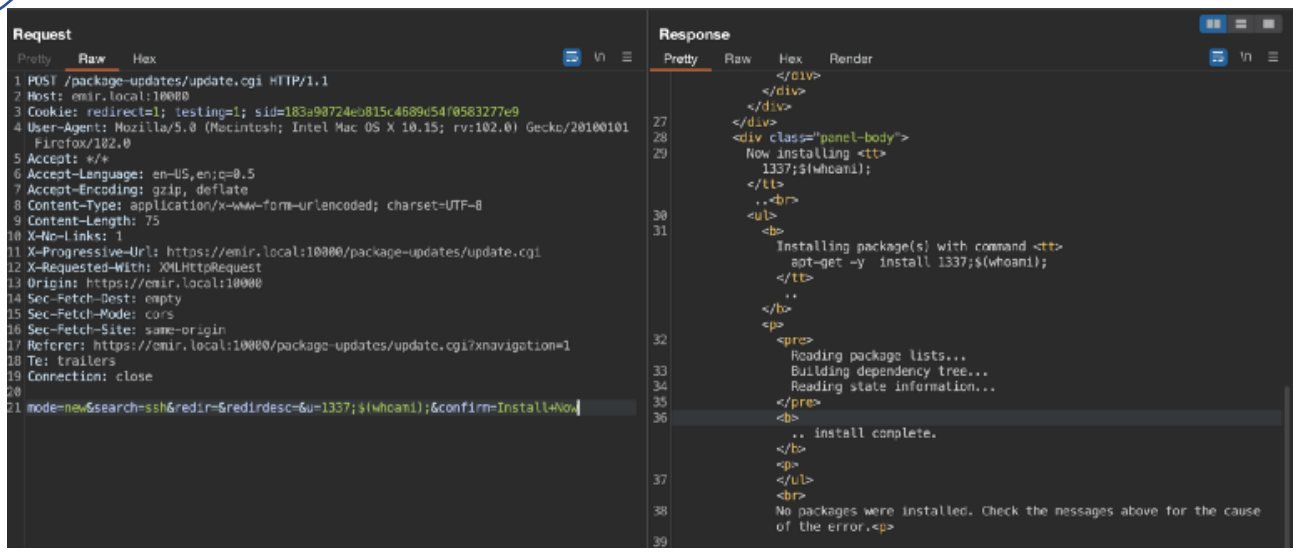
Pada baris 300 ditemukan fungsi "*package_install()*". Dilakukan pemeriksaan lebih detail di mana pada bagian bawah, pengguna dapat melihat bahwa fungsi "*update_system_install()"* dipanggil dengan variabel "$*name*", yang merupakan nama *package* yang diberikan oleh pengguna pada baris 345 (Fungsi tersebut didefinisikan dalam *file* apt-lib.pl). Oleh karena itu, dilakukan pebacaan ulang isi *file* "apt-lib.pl" dan ditemukan fungsi yang relevan.



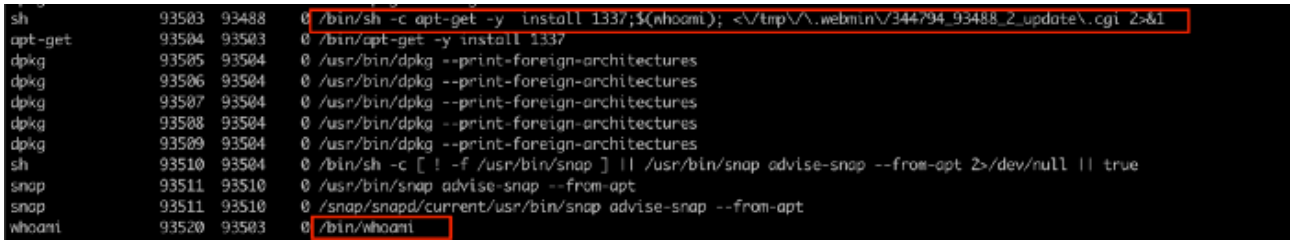
```
15  # Install some package with apt
16  sub update_system_install
17  {
18  local $update = $_[0] || $in{'update'};
19  local $force = !$_[2];
20  local (@rv, @newpacks);
21
22  # Build the command to run
23  $ENV{'DEBIAN_FRONTEND'} = 'noninteractive';
24  $update = join(" ", map { quotemeta($_) } split(/\s+/, $update));
25  $update =~ s/\\(-)|\\(.)/$1$2/g;
26  local $cmd = "$apt_get_command -y ".($force ? " -f" : "")." install $update";
27  print "<b>",&text('apt_install', "<tt>$cmd</tt>"),"</b><p>\n";
28  print "<pre>";
29  &additional_log('exec', undef, $cmd);
30
31  # Run dpkg --configure -a to clear any un-configured packages
32  $SIG{'TERM'} = 'ignore';    # This may cause a Webmin re-config!
33  local $out = &backquote_logged("dpkg --configure -a 2>&1 </dev/null");
34  print &html_escape($out);
35
36  # Create an input file of 'yes'
37  local $yesfile = &transname();
38  &open_tempfile(YESFILE, ">$yesfile", 0, 1);
39  foreach (0..100) {
40      &print_tempfile(YESFILE, "Yes\n");
41      }
42  &close_tempfile(YESFILE);
43
44  # Run the command
45  &clean_language();
46  &open_execute_command(CMD, "$cmd <".quotemeta($yesfile), 2);
```

Gambar 8. */software/apt-lib.pl*

Dilakukan pembacaan ulang fungsi “apt-lib.pl”, dapat dilihat pada baris 18 bahwa parameter pertama dari fungsi (nama *package* yang dikirim pengguna sebelumnya) ditetapkan ke variabel bernama “$*update*”. Kemudian, pada baris 26, dapat dilihat bahwa variabel ini dimasukkan dalam perintah tanpa kontrol apa pun (Misalnya: apt-get -y *install user_controlled_variable*). Pada baris 46, diketahui bahwa perintah yang relevan dieksekusi langsung pada sistem, tanpa mekanisme kontrol apa pun. Oleh karena itu, pengguna dapat menjalankan perintah pada sistem dengan hak akses *root* dengan memberikan parameter "*confirm*" dalam *request* instalasi *package* baru dan memberikan nilai untuk menjalankan perintah pada sistem dalam nama *package*.



Gambar 9. *HTTP Request For Exploit Vulnerability*



Gambar 10. *Commands Running On The System After The Request*.

Panduan Mitigasi

Untuk melakukan pencegahan terhadap kerentanan CVE-2022–36446, melakukan pembaruan dan mengimbau agar seluruh pengguna *Webmin* untuk menggunakan produk yang telah ditingkatkan pada versi 1.997 atau versi terbaru.

Riwayat Dokumen

Versi Dokumen	Tanggal Rilis
1.0	Senin, 22 Agustus 2022

Ketentuan Penggunaan Dokumen

Dokumen Imbauan ini tersedia secara bebas dengan mengakses portal *Website* ID-SIRTII/CC. Terkait penggunaan dokumen imbauan ini, dapat digunakan oleh seluruh pihak yang menggunakan produk terdampak kerawanan yang diulas pada dokumen imbauan ini.

Referensi

[1] "CVE-2022–36446 — Webmin 1.996 — Remote Code Execution (RCE — Authenticated) During Install New Packages" https://medium.com/@emirpolat/cve-2022-36446-webmin-1-997-7a9225af3165 (accessed August. 22, 2022)

[2] “CVE-2022-36446 Detail" https://nvd.nist.gov/vuln/detail/CVE-2022-36446 (accessed August. 22, 2022)

[3] "Webminrce.md" https://gist.github.com/emirpolatt/cf19d6c0128fa3e25ebb47e09243919b (accessed August. 22, 2022)

[4] "CVE-2022-36446" https://www.tenable.com/cve/CVE-2022-36446 (accessed August. 22, 2022)

[5] "Webmin 1.996 - Remote Code Execution (RCE) (Authenticated)" https://www.exploit-db.com/exploits/50998 (accessed August. 22, 2022)

[6] "Webmin Package Updates Command Injection)" https://packetstormsecurity.com/*file*s/168049/Webmin-Package-Updates-Command-Injection.html (accessed August. 22, 2022)

[7] "Webmin Package Updates Command Injection)" https://packetstormsecurity.com/*file*s/168049/Webmin-Package-Updates-Command-Injection.html (accessed August. 22, 2022)

KONTAK KAMI

(021) 788 33610

bantuan70@bssn.go.id

Jl. Harsono RM No. 70, Ragunan
Pasar Minggu, Jakarta Selatan, 12550